CFP Spring Meeting—Privacy & Security Working Group Report

15 April 2010

Karen Sollins & Jim Fenton

Karen's Presentation

The major purpose of this discussion is to report on the work we've been doing on the Social TV case study paper, but more importantly to formulate the next steps of our group's agenda, and we want to draw upon the large group assembled here.

In terms of the Social TV case study paper that our group is working on, we are almost finished, and are drawing some interesting conclusions regarding the composition of identities that potentially occur through the composition of social networking and other platforms to create Social TV experiences.

Looking forward, our group is looking at identity management services as our next focus. There are three major identity providers (Liberty Alliance, OpenID, CardSpace) but there are many. There are

In defining a course of action for our identity management project, we are proposing to begin by surveying existing systems and developing a taxonomy, while also obtaining a set of challenging examples from CFP member organizations to ground our work. We then hope to propose a framework for reasoning about identity systems, and draw some recommendations and conclusions from our study.

Jim's Presentation

Jim's presentation began with an introduction to and background of identity systems and the challenges both in discussing and defining them, as well as thinking about their architecture.

Things to consider about identity systems:

- Not everything is a web transaction. An identity system would be helpful in deciding whether to unlock a door, authorize a vending machine transaction, etc.
- Challenges of user trust: not every users trusts the same entities (governments, banks, trusted corporations/brands)
- Many identity systems are bound tightly to specific authentication methods (again thinking of web transactions), which makes it difficult to optimize the method relative to the risk/value of the transaction
- There are opportunities for identity providers to develop user behavior profiles and flag anomalous behavior (potentially controversial from a privacy standpoint).
- Credential management—a digital key cabinet—is necessary to avoid simple linking of user profiles across relying parties. Directed identity and linking of identities is still possible, and subpoena-able by law enforcement
- Attribute distribution and attestation: what is the best (most trustworthy) source of attributes about an individual's identity, such as credit score, birth date, etc.?
- Attribute trust can result from federation (explicit bilateral relationships) amongst identity providers, or accreditation (implicit multilateral recognition through group membership—scales better)